Facebook y los riesgos de la "descontextualización" de la información

Dumortier, Franck

Published in:
IDP, Revista de Internet, Derecho y Política

Publication date:
2009

Document Version
le PDF de l'éditeur

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

Facebook y los riesgos de la «descontextualización» de la información

Franck Dumortier

Fecha de presentación: julio de 2008
Fecha de aceptación: septiembre de 2008
Fecha de publicación: diciembre del 2009

Resumen

En los últimos años, ha aumentado drásticamente la participación en sitios de redes sociales virtuales (en lo sucesivo, llamados «OSNS»). Servicios como los conocidísimos Facebook y Myspace, u otros como Frienster, WAYN, Bebo, Orkut de Google y muchos más cuentan con millones de usuarios registrados y no dejan de crecer. El modelo más común de estos sitios se basa en la presentación de los perfiles de los participantes y la visualización de su red de relaciones con los demás. Asimismo, las redes OSNS conectan los perfiles de los participantes con sus identidades públicas, usando nombres reales u otros símbolos de identificación del mundo real (como fotos, vídeos, direcciones de correo electrónico, etc.) a fin de permitir la interacción y comunicación entre individuos del mundo real. Por tanto, un sitio como Facebook no se puede considerar únicamente como un patio de recreo para «entes virtuales» en el que las identidades son flexibles y están desconectadas de sus «cuerpos reales». La disposición de información de registro completa, exacta y actualizada por parte de los usuarios no sólo es deseable, sino que es un requisito incluido en las condiciones de uso de Facebook. Este requisito, junto con la misión del servicio de organizar la vida social real de sus miembros, supone un incentivo importante para los usuarios, instándoles a publicar únicamente información real y válida sobre sí mismos. Una vez proporcionada esta información exacta, las interacciones en Facebook implican una amenaza para la privacidad. En este informe, argumento que el principal riesgo para la privacidad en Facebook es el de la «descontextualización» de la información que proporcionan los participantes. En mi opinión, esta amenaza de la «descontextualización» se debe a tres de las características principales de Facebook: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización en la red de Facebook. El fenómeno de «descontextualización» no sólo supone una amenaza para el derecho a la protección de datos, en el sentido del derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho a la privacidad como ser humano: el derecho del ser humano a ser un yo conscientemente múltiple y gregario sin una discriminación injustificada.

Palabras clave

privacidad, protección de datos, redes sociales virtuales, descontextualización de la información

Franck Dumortier
Título original: *Facebook and risks of "de-contextualization" of information*

Tema
Protección de datos y privacidad

Facebook and the Risks of "De-contextualization" of Information

Abstract
Participation in online social networking sites (hereafter OSNS) has increased dramatically in recent years. Services such as the well-known Facebook and Myspace but also Frienster, WAYN, Bebo, Google's Orkut and many others, have millions of registered active users and are continuously growing. The most common model for these sites is based on the presentation of the participants' profiles and the visualisation of their network of relations to others. OSNS also connect participants' profiles to their public identities, using real names and other real-world identification signs (pictures, videos, e-mail addresses, etc.) to enable interaction and communication between real-world subjects. Hence, a site like Facebook cannot be considered purely as a playground for "virtual bodies" in which identities are flexible and disconnected from "real-world bodies". Not only is the provision of accurate, current and complete registration information from the users encouraged, it is even required by Facebook's terms of use. This requirement, along with the service's mission of organizing the real social life of its members, provides major incentives for users to publish only real and valid information about themselves. This accurate information being provided, privacy threats derive from interactions on Facebook. In this paper, I argue that the main privacy risk on Facebook is the one of loss of context of the information spread by users. This de-contextualization threat is due to three major characteristics of Facebook: 1) the simplification of social relations, 2) the high level of information diffusion and 3) the network globalization and normalization effects of Facebook. This loss of context is a risk not only to data protection rights, meaning the right of the individual to control their informational identity presented in a certain context, more fundamentally it threatens the human right to privacy: the right to be a conscious, multiple and relational self not suffering any form of discrimination.

Keywords
privacy, data protection, online social networking, de-contextualization of information

Topic
Privacy and data protection

Introducción

En estos últimos años, se ha observado un aumento continuo en la participación en sitios de redes sociales virtuales (en lo sucesivo, llamados «OSNS»), con una multiplicación exponencial del número de usuarios. Por ejemplo, aunque la audiencia internacional de Facebook ascendió a un total de 20 millones de usuarios en abril de 2007, el número había aumentado hasta 200 millones dos años después, con un promedio de 250.000 nuevos registros diarios desde enero de 2007. La «proporción activa» de la audiencia de Facebook también es impresionante: según las estadísticas publicadas en el sitio web, más de 100 millones de usuarios se registran en Facebook al menos una vez al día, mientras más de 20 millones de usuarios actualizan su configuración a diario, como mínimo.[1] Fundada en febrero de 2004, Facebook desarrolla tecnologías que *«facilitan el intercambio de*

1. Ver estadísticas detalladas en el sitio web de Facebook: http://www.facebook.com/press/info.php?timeline

información a través de un esquema social, el mapa digital de las conexiones sociales de los usuarios en el mundo real».[2] De acuerdo con la definición de danah boyd,[3] Facebook es, por tanto, un «sitio de redes sociales» en el sentido de que es un *«servicio basado en la red que permite a los individuos (1) crear un perfil público o semipúblico dentro de un sistema delimitado, (2) articular una lista de otros usuarios con los que tienen conexión y (3) visualizar y entrecruzar su lista de conexiones y las realizadas por otros dentro del sistema»*.[4] Adicionalmente, la característica principal de un sitio como Facebook es conectar los perfiles de los participantes con sus identidades públicas, usando nombres reales y otros modos de identificación del mundo real como fotografías, vídeos o direcciones de correo electrónico, permitiendo así la interacción y comunicación entre individuos del mundo real. Por tanto, Facebook está muy lejos de equipararse a los espacios de chat con pseudónimo y no se puede considerar únicamente como un patio de recreo para «entes virtuales» en el que las identidades son flexibles y están desconectadas de sus «cuerpos reales». De hecho, no hay casi nada «virtual» en lugares como Facebook. La disposición de información de registro exacta y actualizada por parte de los usuarios no sólo es deseable, sino que es un requisito incluido en las condiciones de uso. De hecho, Facebook obliga a sus usuarios a *«indicar sus nombres e información reales»*, a mantener su *«información de contacto exacta y actualizada»* y les prohíbe *«incluir información personal falsa»*.[5] Estos requisitos, junto con la misión del servicio de organizar la vida social real de sus miembros, suponen un incentivo importante para los usuarios, instándoles a publicar únicamente información real y válida sobre sí mismos. Las estadísticas son elocuentes: ya en 2005, el 89% de los perfiles de Facebook usaban nombres reales, mientras el 61% de los perfiles incluían imágenes que permitían una identificación directa.[6]

Según las estadísticas de Facebook, cada mes, se cargan más de 850 millones de fotos y 8 millones de vídeos. Además, cada semana se comparten más de 1.000 millones de unidades de contenido (enlaces en la red, noticias, entradas de blogs, notas, fotos, etc.). Dada la difusión del uso e intercambio de información personal considerada exacta y actualizada, existen importantes amenazas a la privacidad que pueden derivarse de las interacciones en Facebook, siendo la principal el riesgo de «descontextualización» de la información que aportan los participantes. En mi opinión, esta amenaza de la «descontextualización» se debe a tres de las características principales de Facebook: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización en la red de Facebook. El riesgo de «descontextualización» no sólo supone una amenaza para el derecho a la protección de datos, es decir, el derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho a la privacidad como ser humano: el derecho del ser humano a ser un yo múltiple y gregario sin una discriminación injustificada.

En la primera parte, examino las distintas características de Facebook que suponen un riesgo de «descontextualización» de la información en circulación. En la segunda parte, se explica por qué este fenómeno de descontextualización es una amenaza tanto para los derechos de privacidad como para la protección de datos. Finalmente, expongo que la protección de la privacidad y de los datos en Facebook no se debe centrar únicamente en las soluciones y penalizaciones para los individuos agraviados, sino en el diseño de una arquitectura que rija los flujos de datos en múltiples contextos en el sitio. Dada la importancia de la amenaza de la «descontextualización», la arquitectura de Facebook debe estar diseñada de modo que evite cualquier interferencia tanto con el derecho a la pri-

2. *Ibidem*.
3. danah boyd no escribe su nombre con mayúsculas.
4. D. BOYD; N. ELLISON (2007). «Social Network Sites: Definition, History, and Scholarship». *Journal of Computer-Mediated Communication*, vol 1, n.º 13, art. 11. Disponible en línea en: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Boyd y Ellison usan «sitio de redes sociales» en lugar de «sitio de establecimiento de redes sociales» porque «los participantes no necesariamente están "estableciendo contactos" ni tratando de conocer a otras personas; en su lugar, suelen comunicarse con personas que ya forman parte de su red social más amplia».
5. Véase la «Declaración de derechos y responsabilidades» de Facebook, en: http://www.facebook.com/terms/spanish.php
6. R. GROSS; A. ACQUISTI (2005). «Information Revelation and Privacy in Online Social Networks». En: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. Pág.77.

vacidad como con la protección de datos, siempre que dicha interferencia no sea estrictamente necesaria en un estado democrático.

1. Los riesgos de la descontextualización que se derivan de las interacciones en Facebook

En este informe, uso el término «descontextualización» para conceptualizar lo que ocurre cuando se usan comportamientos o información en un contexto distinto de aquél para el que se crearon. Tal como indica Nissembaum, el fenómeno de la descontextualización surge cuando los individuos no respetan las normas de distribución y adecuación contextuales.[7] Por ejemplo, cuando un comportamiento que sería adecuado con un amigo íntimo en un bar se muestra en público o en el trabajo, viola las normas contextuales de adecuación. Del mismo modo, si mi superior llega a conocer información dirigida originalmente a mi novia, viola las normas contextuales de distribución. Lo verdaderamente problemático en estas normas contextuales es que no admiten una definición precisa, ya que se derivan de una apreciación personal sobre el modo en que debería circular la información en el mundo físico, o, en este contexto, en el «mundo real». De hecho, ambas normas de adecuación y distribución presuponen cierto entorno situacional, ya que el modo en que se divulga la información depende de propiedades muy determinadas de ese entorno, como sus características arquitectónicas, temporales e interpersonales.[8] A modo de ejemplo, no me comportaría del mismo modo con mi jefe en un bar a las 10 de la noche que en el trabajo a las 8 de la mañana, ni revelaría la misma información a las 10 de la noche en ese mismo bar con mi jefe si mi madre se uniera al grupo. Por tanto, en el mundo físico, las normas contextuales de distribución y adecuación se basan en algo típicamente humano: los sentimientos.

No obstante, como explicaré en las próximas secciones, Facebook tiene un diseño completamente distinto al del mundo físico, y sus propiedades arquitectónicas, temporales e interpersonales tienen el potencial de generar una asimetría entre los «sentimientos» de los usuarios y el modo en que se propaga la información. Por tanto, el uso del concepto de «descontextualización» es particularmente interesante en el caso de Facebook, ya que se trata de un entorno *«en el que los mundos entran en colisión, donde las normas quedan atrapadas en el fuego cruzado entre comunidades, donde se derriban los muros que separan las distintas situaciones sociales»*.[9]

En las siguientes secciones, expondré que la amenaza de la descontextualización en Facebook se debe a tres de sus características principales: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización de Facebook.

1.1. La simplificación de las relaciones sociales en las OSNS

Según las estadísticas publicadas en Facebook, un usuario medio tiene 120 «amigos» en el sitio. Ello implica que, cuando un usuario actualiza su perfil (cargando una foto o un vídeo, modificando su ideología política o creencias religiosas o cambiando su situación sentimental), publica un mensaje en su «muro» o responde a un test, esta información queda, por defecto y de media, a disposición de más de cien personas con las que el usuario mantiene distintos tipos de relación. De hecho, las personas con que se relaciona un usuario en Facebook pueden ser tan variadas como miembros de su familia, colegas, amantes, amigos reales, conocidos en un bar, antiguos compañeros de escuela e incluso desconocidos. Los teóricos de las redes sociales han debatido sobre la relevancia de las relaciones a distintos niveles de profundidad e intensidad en la red social de una persona.[10] Cabe destacar el hecho de que la

7. Véase H. NISSENBAUM (2004). «Privacy as Contextual Integrity». *Washington Law Review*, vol. 79, n.º 1.
8. C. PETERSON formuló esta misma idea en (2009). «Saving Face: The Privacy Architecture of Facebook» (borrador para comentarios – primavera de 2009). *The Selected Works of Chris Peterson*. Pág. 9. Disponible en: http://works.bepress.com/cpeterson/1
9. Véase C. PETERSON (2009). «Saving Face: The Privacy Architecture of Facebook» (borrador para comentarios – primavera de 2009). *Op.cit*, resumen.
10. Véase, por ejemplo, M. GRANOVETTER (1973). «The strength of weak ties». *American Journal of Sociology*, núm. 78, pág. 1360-1380. Véase también M. GRANOVETTER (1983). «The strength of weak ties: A network theory revisited». *Sociological Theory*, n.º 1, pág. 201-233. Strahilevitz ha destacado la relevancia de esta teoría sobre la privacidad. Véase L. J. STRAHILEVITZ (2005). «A social networks theory of privacy». *University of Chicago Law Review*, vol. 72, pág. 919.

aplicación de la teoría de las redes sociales a la revelación de información saca a la luz diferencias significativas entre los escenarios real y virtual (offline y online). En el mundo real, la relación entre divulgación de la información y la red social de una persona tiene, tradicionalmente, múltiples facetas: *«En ciertas ocasiones, queremos que la información sobre nosotros esté sólo a disposición de un pequeño grupo de amigos íntimos, y no de desconocidos. En otros casos, estamos dispuestos a revelar información personal a extraños, pero no a quienes nos conocen bien»*.[11] Por ende, las redes sociales reales están formadas por lazos definibles de un modo impreciso como lazos fuertes o débiles, pero en realidad estos lazos son extremadamente diversos en lo referente al grado de cercanía e intimidad con que un sujeto percibe una relación. Las redes sociales virtuales, por otro lado, suelen reducir estas relaciones llenas de matices a relaciones binarias simplistas: «Amigo o no». En su estudio de las redes sociales virtuales, danah boyd observa que *«no hay ninguna forma de determinar qué escala se ha usado o cuál es el papel o el peso de la relación. Aunque algunos usuarios están dispuestos a marcar a cualquiera como Amigo, y otras prefieren una definición conservadora, la mayoría de los usuarios tienden a incluir en esta lista a todos aquellos a los que conocen y que no les disgustan. A menudo, esto supone que se clasifica como Amigos incluso a personas a las que el usuario no conoce o en las que no confía particularmente»*.[12]

Cada vez más, los usuarios de Facebook tienden a clasificar como *«Amigos»* a todas aquellas personas a las que no odian[13], y compartirán con estas relaciones una cantidad increíble de datos que podrían ser inadecuados en el contexto *heterotópico*[14] de Facebook. Tomemos, por ejemplo, a un usuario de Facebook que tiene 100 «Amigos»: 4 de ellos son parientes, 16 son «amigos íntimos», 1 amante, 4 ex amantes, 30 antiguos compañeros de colegio, 30 conocidos (de distintos contextos), 14 compañeros de trabajo y su jefe. Ahora imaginemos que nuestro usuario instala una aplicación ajena en Facebook para responder a un test divertido «¿Eres alcohólico?» y al mismo tiempo cambia su «situación sentimental» a soltero. No hay duda de que la combinación de estas informaciones tendrá un significado distinto para sus amigos y su pareja que para sus colegas, su jefe o su madre. De estas observaciones, se deriva una amenaza de descontextualización: la dificultad que tiene un ente con múltiples facetas para restringir la información que desea compartir con «Amigos» de distintos contextos. Simplificando, responder a un test «¿Cuál es tu postura sexual favorita?» puede proporcionar información interesante a mi novia pero seguramente *no será adecuada* para ninguno de mis compañeros de trabajo.

En este sentido, hay un punto de partida en el elemento «Listas de amigos» que proporciona Facebook y que permite a los usuarios organizar a sus amigos en distintas categorías. La herramienta les permite incluir y excluir a grupos de amigos de la posibilidad de ver partes de su perfil y contenidos. En nuestro ejemplo, un usuario cuidadoso podría agrupar a cada tipo de «amigos» en distintas categorías que haya predefinido y darles distintos niveles de acceso a informaciones tales como fotos, vídeos, situación, mensajes, etc. Sin embargo, al resolver en parte el problema de la limitación del acceso a determinadas informaciones añadiendo un control más específico, Facebook también ha introducido una mayor complejidad y trasfondo conceptual para los usuarios: ahora tienen que «clasificar» a sus «amigos». Este es exactamente el motivo por el que no se puede considerar que las «Listas de amigos» imiten exactamente el modo en que todos limitamos el acceso de determinados amigos a cierta información personal en el mundo real. De hecho, el elemento se parece mucho más al modo en que el administrador de un sistema podría configurar las autorizaciones de uso de los recursos de un ordenador que al modo en que se desarrollan los procesos de divulgación de la informa-

11. R. GROSS; A. ACQUISTI, «Information Revelation and Privacy in Online Social Networks». Actas del *2005 ACM Workshop on Privacy in the Electronic Society*. Pág. 81.
12. D. BOYD (abril, 2004). «Friendster and publicly articulated social networking». En: *Conference on Human Factors and Computing Systems* (*CHI 2004*). Austria: Viena. Pág. 2.
13. Nótese que Hatebook.org, la versión antagónica de Facebook, se define como «*una herramienta antisocial que te desconecta de todo lo que odias*».
14. Para obtener más detalles sobre Facebook como espacio heterotópico, véase la sección 2.1, pág. 11.

ción en la vida cotidiana: el «etiquetado» de amigos y la creación de «Listas de amigos» no son hechos conscientes en el mundo real.

Por tanto, la simplificación de las relaciones sociales en OSN lleva implícita una primera amenaza de descontextualización de la información teniendo en cuenta que las relaciones binarias en estos sitios pueden provocar incumplimientos de las normas contextuales de adecuación o de distribución: la divulgación de la información nunca estará tan fragmentada en el mundo virtual como lo está en el mundo real.

1.2. La amplia difusión de la información inherente a las interacciones en Facebook

No sólo la simplificación de las relaciones sociales en Facebook implica una amenaza de descontextualización, también el modo en que la información se puede difundir ampliamente a lo largo del entramado social. En el mundo real, es excepcionalmente improbable que la información sobre una persona sea interesante a más de dos grados de información. En estas situaciones, Duncan Watts observa que *«cualquiera que se encuentre a mayor distancia que un amigo de un amigo es, a todos los efectos, un desconocido... Todo lo que se sitúe a más de dos grados podría estar perfectamente a mil grados de distancia»*.[15] En otras palabras, al menos en la era anterior a Facebook, a nadie le importaban demasiado las personas que se apartaban a más de dos grados de nosotros. Strahilevitz lo ilustra perfectamente en la siguiente cita:

«Las aventuras extramatrimoniales son actos fascinantes. Dicho eso, ninguna persona decente iría a un cóctel y le contaría una historia íntima sobre el amigo del amigo de un amigo que está teniendo una relación adúltera con alguien a quien ni hablante ni oyente conocen. Sólo si el hablante o el oyente sabe quiénes son los adúlteros o si los detalles del caso son especialmente sórdidos, divertidos o memorables, será probable que la información se difunda más allá por la red social. Y para cuando la información haya recorrido toda la cadena, parece probable que los nombres de los implicados hayan desaparecido de la historia.»[16]

Así, cuando se trate de hechos transmitidos oralmente de persona en persona, alguien debería tener una «expectativa razonable de integridad contextual» a más allá de dos grados en una red social. Esta norma lógica parece no sustentarse tan bien cuando uno se aleja de las comunicaciones del mundo real e interactúa en servicios de redes virtuales como Facebook, por cinco razones principales.

La primera es que la difusión de la información a lo largo del esquema social se ve impulsada por la presencia de una red visible de amigos en el perfil de cada participante. Mientras en el mundo real los amigos pueden pasar años sin saber que comparten un amigo mutuo, en Facebook pueden averiguar con gran facilidad quiénes son sus amigos comunes. Esta lista también hace que sea más fácil para todos saber quiénes son los amigos del amigo de un amigo propio. Además, cada perfil de la lista de amigos de un amigo se puede «compartir» y comentar en el perfil del usuario. A modo de ejemplo, yo puedo ojear mi lista de relaciones, elegir a uno de mis amigos, ver quiénes son sus amigos, después pasar a los amigos de sus amigos y finalmente publicar el perfil limitado de uno de ellos en mi perfil con un comentario desafortunado que se puede seguir compartiendo y comentando a lo largo de los esquemas sociales de mis propios «amigos».

En segundo lugar, Facebook está formado por miles de redes en todo el mundo, y se anima a los usuarios a unirse a ellas para conocerse y hacer amigos entre las personas de su área. Las mayores de estas redes son las conocidas como «redes geográficas», de las que la belga aúna a más de 780.000 personas. Una vez se une a una de estas redes, un usuario puede «clasificar» a los usuarios de la misma red usando criterios como el sexo, la edad, la situación sentimental, sus intereses o su ideología política. Además, dependiendo de la configuración de privacidad de la persona objetivo, los usua-

15. D. J. WATTS. *Six Degrees: The Science of a Connected Age*. Nueva York: Norton. Pág. 299-300.
16. L. J. STRAHILEVITZ. *Op.cit*. Pág. 47.

rios pueden acceder a la totalidad o a parte de los perfiles de los amigos de los amigos de sus amigos.[17]

Otro factor que podría causar una amplia difusión de la información es la opción de «etiquetado» que propone Facebook. Una etiqueta es una palabra clave, a menudo el nombre real de un participante asociado o asignado a una unidad de información (una foto, un vídeo, etc.) para describir al individuo y permitir una clasificación y la búsqueda de información sobre la base de la palabra clave. Cuando se asocial a una foto o a un vídeo, la etiqueta proporciona un acceso directo al perfil del usuario representado. Aquí aparece el clásico problema de Facebook: bajas la guardia durante unas horas en una noche (o un día) y alguien cuelga las fotos (o vídeos) del momento para que las vean todos los amigos de un amigo, no sólo tus amigos íntimos que compartieron ese momento contigo. De hecho, Facebook no ha creado un ajuste de privacidad por defecto que permita a los usuarios aprobar o rechazar etiquetas de fotos antes de que puedan aparecer en el sitio.[18]

Una cuarta preocupación por la difusión involuntaria de información se deriva de la «Plataforma Facebook desde el móvil». Según las estadísticas de Facebook, *«actualmente hay más de 30 millones de usuarios activos que acceden a Facebook a través de sus dispositivos móviles.. Los usuarios que usan Facebook en sus dispositivos móviles son casi un 50% más activos en Facebook que los usuarios de otros tipos de equipos»*.[19] La mayor amenaza para la privacidad que implica esta herramienta se deriva de la ubicuidad de los dispositivos móviles, que tienen el potencial de permitir que la información virtual acceda al mundo real en cualquier momento, en cualquier lugar y en cualquier ocasión. De hecho, en el mundo real no importan los ajustes de privacidad: con su móvil, uno de mis amigos del mundo real podría mostrarme fácilmente el perfil completo en Facebook de uno de sus «amigos», al que no conozco en absoluto, sólo porque una de sus características es interesante en el contexto de nuestra conversación personal.

Por último, la introducción de aplicaciones de terceros en Facebook ha expuesto los datos personales de los usuarios ante un grupo creciente de diseñadores y comercializadores. Según un estudio realizado en 2007,[20] de las 150 aplicaciones principales de Facebook, cerca del 91% tenía acceso a datos personales innecesarios. Dada la naturaleza recreativa de muchas aplicaciones principales, probablemente esta estadística no ha cambiado drásticamente. Los usuarios se han acostumbrado a autorizar incluso aplicaciones simples y no saben qué datos se van a usar y a quién se van a transferir antes de autorizar una aplicación. «We're Related» *(somos familia)* es una de estas aplicaciones ajenas fuente de estas preocupaciones. Según un informe, esta aplicación, que dice tener 15 millones de usuarios activos cada mes, trata de identificar y enlazar a miembros de una familia que ya estén en la red, aunque su parentesco sea muy lejano: *«Se solicita a los nuevos usuarios que den carta blanca a la aplicación para que "acceda a su información del perfil, fotos, la información de sus amigos y todos los contenidos que requiera para funcionar". La aplicación parece autorizarse a sí misma para proporcionar esta información a cualquier otro participante de Facebook – aunque los usuarios hayan establecido unos parámetros de privacidad*

17. En 2007, la empresa de seguridad y control de TI, Sophos, reveló que los miembros exponían imprudentemente sus datos personales de forma masiva a millones de extraños, exponiéndose ellos mismos a un riesgo de robo de identidad. La empresa de seguridad realizó una elección aleatoria de 200 usuarios en la red de Facebook en Londres, que es la mayor red geográfica del sitio, con más de 1,2 millones de miembros, y detectó que un impresionante 75 por ciento permitió que cualquiera visionara su perfil, independientemente de si lo habían puesto o no a disposición de sus amigos. Sophos vió evidencias de que los usuarios de Facebook en otras regiones geográficas exhiben de un modo similar su información personal ante perfectos desconocidos. La razón de esta divulgación involuntaria de la información era que, aun cuando se hubiera configurado previamente el grado de privacidad para asegurarse de que sólo los amigos accedieran a la información, al unirse a una red, el perfil se abría automáticamente a cualquier otro miembro de la red. Hasta 2009, Facebook no cambió su configuración de identidad por defecto para las redes geográficas a fin de evitar la exposición involuntaria de los perfiles.
18. Existe la posibilidad de restringir indirectamente la visibilidad de las fotos etiquetadas visitando primero la página de privacidad de tu perfil y modificando el parámetro junto a «Fotos en las que se te ha etiquetado», eligiendo la opción «Personalizar» y después la opción «Sólo yo» y «Ninguna de mis redes». Si deseas que las fotos etiquetadas sean visibles para ciertos usuarios, puedes incluirlos en el cuadro bajo la opción «Algunos amigos». En el cuadro que aparece después de elegir «Algunos amigos», puedes introducir a amigos individuales o listas de amigos.
19. Véanse las estadísticas de Facebook en: http://www.facebook.com/press/info.php?statistics
20. A A. FELT; D. EVANS (mayo, 2008). «Privacy Protection for Social Networkin APIs». *W2SP*. Disponible en http://www.cs.virginia.edu/felt/privacybyproxy.pdf

más estrictos a fin de limitar el acceso a sus datos personales.»[21] Sin embargo, tal como se indica en los términos de uso de Facebook, la empresa no asume ninguna responsabilidad por las prácticas inadecuadas acerca de la privacidad de los diseñadores de aplicaciones externas.[22]

Combinados, estos cinco factores implican un riesgo de difusión involuntaria de los datos más allá de las «expectativas razonables de integridad contextual» de los usuarios de Facebook, ya que la información importante compartida con sus «amigos» puede propagarse más allá de dos niveles de conexión.

En la siguiente sección, expondré que esta amenaza de descontextualización puede verse incrementada por los efectos de globalización y normalización de Facebook.

1.3. Los efectos de globalización y normalización de Facebook

Todos hemos experimentado el incremento en la presión de nuestras relaciones para que nos hagamos por fin con el programa y nos unamos a la red. En parte, se puede explicar por el hecho de que cuando alguien se registra en Facebook, el sitio invita al nuevo usuario a *«averiguar cuáles de sus contactos por email están ya en Facebook»*. Entonces Facebook pide a los usuarios que introduzcan su dirección de email y contraseña para muchos de los principales proveedores de servicios de correo electrónico (Yahoo, Hotmail, Gmail, etc.). A continuación, Facebook se registra en la cuenta y se descarga todos los contactos. Los usuarios ven una lista de los individuos que actualmente son miembros de Facebook, y tienen la posibilidad de enviar solicitudes de amistad a cada uno de ellos. Aparece una pantalla con todos los contactos preseleccionados. Ahora, el usuario tiene la opción de invitar a todos sus otros contactos a unirse a Facebook.[23] Por defecto, se preseleccionan todos los contactos: por tanto, el comportamiento por defecto es enviar mensajes a todos los contactos invitándoles a ser amigos en Facebook.

Los incentivos para unirse al programa se concretan aún más cuando se examina la función de «etiquetado» propuesta por Facebook. Un elemento problemático de esa función es que se puede etiquetar a personas que no se hayan registrado en la red (por tanto, a los denominados amigos, a perfectos desconocidos e incluso a enemigos). Por supuesto, se puede ejercer el derecho de acceso y el derecho de rectificación/borrado si alguien desea eliminar una etiqueta en particular de uno mismo, pero primero debe registrarse en Facebook. Esto es lo que podríamos denominar el efecto de globalización de Facebook: sin estar en el programa, uno puede ser un objeto de datos definido por fotos y artículos. Incluso sin conocerlo y sin ser capaz de reaccionar, uno puede ser un tema de conversación ampliamente difundido y bien documentado. Para convertirse en un individuo de datos reales, el objeto de los datos debe registrarse en Facebook antes de poder ejercer sus derechos de protección de datos. Para poder ser actores activos en el control de su identidad informativa, los usuarios están obligados a registrarse en el programa.

Dado el impresionante crecimiento de Facebook (314% el año pasado), el servicio se está convirtiendo, cada vez más, en una herramienta de comunicación diaria, en la que, por ejemplo, está registrado el 21% de la población belga.[24] Paradójicamente, cada vez es más raro no estar en Facebook que lo contrario. Esto es lo que podríamos denominar el efecto de normalización de Facebook: un futuro en que los empresarios se pregunten lo siguiente: *«¿por qué el Sr. X no está en Facebook? Es raro... ¿tiene algo que ocultar?»*, quizá no sea tan lejano.

21. Véase R. WATERS (2009). «Facebook applications raise privacy fears». *Financial times online*. Disponible en http://www.ft.com/cms/s/0/2a58acfa-5c35-11de-aea3-00144feabdc0.html
22. Véanse los Términos de Uso de las Aplicaciones de la Plataforma Facebook: «Cuando instala una Aplicación de Desarrollador, o Developer Application, entiende que dicha Aplicación no ha sido aprobada, asignada ni revisada en modo alguno por Facebook, y que no somos responsables de su uso o incapacidad de uso de tales aplicaciones, incluyendo, sin limitación, el contenido, la exactitud o fiabilidad de dicha Aplicación de Desarrollador ni las prácticas de privacidad u otras políticas del Desarrollador. USE ESTAS APLICACIONES DE DESARROLLADOR POR SU CUENTA Y RIESGO». Disponible en: http://developers.facebook.com/user_terms.php
23. Véase http://epic.org/privacy/facebook/
24. Véanse las estadísticas en http://katrin-mathis.de/wp-mu/thesis/

Una vez descritas las tres características principales de Facebook que implican un riesgo de descontextualización de la información personal, en la siguiente sección, analizaré las consecuencias de tal amenaza respecto a los derechos de privacidad y protección de datos.

2. Consecuencias de la amenaza de descontextualización sobre los derechos a la privacidad y a la protección de datos

Las tres características de Facebook que he presentado – 1) simplificación de las relaciones sociales, 2) amplia difusión de la información y 3) efectos de globalización y normalización – pueden implicar riesgos importantes de descontextualización de la información. Tal amenaza de descontextualización de la información personal en Facebook puede afectar tanto al derecho a la privacidad como al derecho a la protección de datos de los usuarios del servicio.

Las conexiones entre ambos derechos ya han sido objeto de rigurosos análisis por parte de autores de renombre.[25] A los efectos de nuestro debate, tomemos como punto de partida el mero hecho de que el derecho a la privacidad se ha considerado tradicionalmente un «Derecho humano» reconocido a los seres humanos, mientras el «derecho a la protección de datos» se concede a los «sujetos de datos» a través de los instrumentos legales más significativos a escala europea. De hecho, aunque la privacidad y el Tribunal Europeo de los Derechos Humanos giran en torno al ser humano, la directiva 95/46 habla de sujetos de datos. *¿Por qué?* La cuestión podría parecer simplista o trivial, pero entender desde este punto de vista los significados respectivos del derecho a la privacidad y a la protección de datos nos podría ayudar, en mi opinión, a entender el modo en que la descontextualización de la información supone una amenaza para ambos derechos.

2.1. Consecuencias de la amenaza de la descontextualización sobre la Privacidad como un derecho del ser humano

Cabe recordar que la privacidad es un derecho otorgado a los seres humanos y puede parecer trivial, sin embargo, el término «Humano» es extremadamente ambiguo y ha experimentado una extraordinaria evolución histórica y filosófica. A fin de presentar adecuadamente este tema y evitar debates innecesarios, limitémonos a reconocer que un ser humano no se puede reducir a un cuerpo o a una persona física. Naturalmente, en un estado ideal, deberían concederse derechos humanos a todos los cuerpos con especificaciones humanas definidas por la anatomía, pero, históricamente, no cabe duda de que los legisladores también estaban influidos por las concepciones filosóficas del «ser interior» cuando diseñaron el marco de los derechos humanos. A modo de ejemplo, el artículo 1 de la Declaración Universal de los Derechos Humanos define al ser humano como *«dotado de razón y conciencia»*, recuperando un punto de vista muy kantiano según el cual la característica definitiva del ser humano era su capacidad de raciocinio. La razón, según Kant, permitía al ser entender y ordenar el mundo con certeza. En consecuencia, el yo kantiano se concebía como un pilar de identidad de subjetividad coherente, que sobresale en la corriente de la experiencia cambiante. No obstante, la noción modernista liberal del yo como un individuo unitario, estable y transparente ha sido objeto de una crítica cada vez más intensa a lo largo del siglo veinte. De hecho, muchas teorías del modernismo tardío o postmodernistas sobre el yo afirman que es múltiple y fraccionado. En consecuencia, el yo es una noción ilusoria interpretada como algo estático y unitario, pero completamente fluida en la realidad.[26] La evolución de estas reflexiones ha llevado a conceptos del ser humano como un «*yo múltiple*»[27] *relacional, subjetivo y dependiente del contexto*. La idea de Goffman, llena de matices, de una «persona cosmopolita» refleja perfectamente el debate filosófico entre unificación y fragmentación del yo moderno que evoluciona constantemente en una pluralidad de contextos. Según él,

25. Gutwirth y De Hert, por ejemplo, han debatido la distinción considerando el derecho a la privacidad como una especie de «*herramienta de opacidad*» mientras, según los autores, el derecho a la protección de datos sería una «*herramienta de transparencia*». Véase S. GUTWIRTH; P. DE HERT (2006). «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power». En: E. CLAES; A. DUFF; S. GUTWIRTH (eds.) (2006). *Privacy and the criminal law*. Amberes: Intersentia. Págs. 61-104.

«En muchas situaciones modernas, los individuos se ven atrapados en una variedad de contextos dispares... cada uno de los cuales puede requerir diferentes formas de comportamiento «adecuado»... Cuando el individuo sale de un contexto y entra en otro, ajusta la «presentación del yo» con relación a lo que se requiere en una situación particular. A menudo, se piensa que este punto de vista implica que un individuo tiene muchos yos, al igual que existen contextos de interacción divergentes... Sin embargo, no sería correcto ver la diversidad contextual como algo que simple e inevitablemente promueve la fragmentación del yo, y mucho menos su desintegración en múltiples «yos». En muchas circunstancias, incluso puede promover una integración del yo... Una persona puede usar la diversidad para crear una identidad propia distintiva que incorpore de forma positiva elementos de distintas situaciones en un discurso integrado. Por tanto, una persona cosmopolita es precisamente la que logra sentirse a gusto en una variedad de contextos.»[28]

Más allá del dilema postmoderno entre unificación y fragmentación del yo, lo importante a los efectos de nuestro debate es el hecho de que los seres humanos son concebidos, cada vez más, como seres contextuales en constante reinvención de sí mismos, que adoptan distintos papeles, posturas y actitudes en una compleja red de redes abierta a los demás. Teniendo en cuenta esta evolución conceptual del yo humano hacia un yo contextual, es interesante analizar la evolución del significado de su derecho a la privacidad.

Desde su aceptación como *«derecho a ser dejado en paz»*,[29] el derecho a la privacidad ha experimentado evoluciones significativas. Es interesante que el Tribunal Europeo de Derechos Humanos haya afirmado que sería demasiado restrictivo limitar la noción de «vida privada» a un «círculo interior» en el que el individuo puede vivir su propia vida personal del modo que elija y excluirse en él de todo el mundo exterior no incluido en ese círculo: *«El respeto por la vida privada también debe incluir hasta cierto punto el derecho a establecer y desarrollar relaciones con otros seres humanos»*.[30] Naturalmente, ahora la privacidad se concibe como un fenómeno que tiene en cuenta las relaciones entre un yo y su entorno/otros yos. Como observa Fried,

«La privacidad no es sólo un medio posible entre muchos de asegurar otro valor, sino que está necesariamente relacionada con los fines y las relaciones del tipo más fundamental: respeto, amor, amistad y confianza. La privacidad no sólo es una buena técnica de continuación de estas relaciones fundamentales, que son más bien inconcebibles sin privacidad. Requieren un contexto de privacidad o la posibilidad de gozar de privacidad para existir.»[31]

Además, dado que los «*usuarios tienen, y es importante que mantengan, diferentes relaciones con usuarios diferentes*»,[32] las relaciones entre los yos son, por naturaleza, extremadamente contextuales. Por tanto, Nissenbaum afirmó que el valor definitivo que debe proteger el derecho a la privacidad es la «integridad contextual»[33] de un yo contextual dado con diferentes comportamientos y que comparte información diferente en función del contexto en el que evoluciona. A este respecto, Rachels observa que:

«Hay una cercana relación entre nuestra capacidad de controlar quién tiene acceso a nosotros y a la información sobre nosotros y nuestra capacidad de crear y mantener

26. Véase, por ejemplo, K. P. EWING (1990). «The Illusion of Wholeness: Culture, Self, and the Experience of Inconsistency». *Ethos*, vol. 18, n.º 3, págs. 251-278 (donde se argumenta que los usuarios «proyectan múltiples representaciones incoherentes de sí mismos que dependen del contexto y pueden variar rápidamente»); A. P. HARRIS (1996). «Foreword: The Unbearable Lightness of Identity». *Berkeley women's law journal*, vol. 11, págs. 207-211 (donde argumenta que el problema con cualquier teoría general de la identidad «es que la "propia identidad" tiene poca sustancia»); J. WICKE (1991). «Postmodern Identity and the Legal Subject». *University of Colorado Law Review*, vol. 62, págs. 455-463 (donde se observa que un concepto postmodernista de la identidad reconoce el yo como fragmentado y captura «sus grietas causadas por la miríada de discursos sociales que lo conforman»).
27. Véase, p. ej. J. ELSTER (1986). «The Multiple Self». *Studies in Rationality and Social Change*. Cambridge University Press.
28. GOFFMAN, citado en A. GIDDENS (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press. Pág. 189.
29. WARREN y BRANDEIS (1890). «The right to privacy». *Harvard Law Review*, vol. 4, n.º 5.
30. Véase, p. ej. ECHR (dic, 1992). *Niemietz v. Germany*. N.º A 251-B, § 29.
31. C. FRIED (1968). «Privacy». *Yale Law Journal*, n.º 77, págs. 475-493.
32. F. SCHOEMAN (1984). «Privacy and Intimate Information». *Philosophical Dimensions of Privacy: an anthology*. Pág. 403-408.
33. H. NISSENBAUM. *Op.cit.*.

diferentes tipos de relaciones sociales con usuarios diferentes... es necesario tener privacidad si vamos a mantener la variedad de relaciones sociales con otros usuarios que queremos tener y por eso es importante.»[34]

Análogamente, Agre definió el derecho a la privacidad como *«la ausencia de límites no razonables en la construcción de la identidad propia»*.[35] Dado que la construcción de la identidad de uno se concibe cada vez más como una integración autonómica y narrativa progresiva de distintos elementos derivados de una diversidad contextual, muchos autores tienden a considerar el derecho a la privacidad como un «derecho a la autodeterminación», una condición importante para la autonomía individual.[36] En otras palabras, al igual que las relaciones con los demás son esenciales para construir la personalidad de un individuo, el derecho a la privacidad también impulsa el propio desarrollo[37] al proteger una serie de relaciones contextualizadas de intrusiones o fugas no razonables. En esta perspectiva, el derecho a la privacidad se puede concebir como «un derecho a la autodeterminación del yo contextual» que le garantiza la posibilidad de actuar y comunicarse como desee *contextualmente* sin tener que temer una *descontextualización* inadecuada de sus comportamientos o de la información.

Imaginemos un padre de 45 años que trabaja como empleado en un banco, participa políticamente en un partido antimilitarista de izquierdas, va a cazar los sábados con sus amigos, va a la iglesia todos los domingos con su familia y le gusta examinar el *Playboy* los lunes con unos amigos durante el descanso matinal. Cabría pensar que algunas de estas representaciones del yo dependientes de un contexto son incoherentes o incompatibles entre sí. También es fácil imaginar cuán inadecuado puede parecer un comportamiento o una información de uno de estos contextos en otro de los contextos dados. Pero, lo que es más fundamental, todos estaremos de acuerdo en que ninguno de estos contextos o situaciones son ilegales o nocivos *per se*. Este es exactamente el objeto del derecho a la privacidad: mostrar *respeto* por la autonomía individual, aunque la construcción de la identidad intercontextual de alguien nos pueda parecer incoherente. Desde este punto de vista, el derecho a la privacidad no sólo es una condición importante de la autonomía individual sino, en un sentido más general, de la supervivencia de una democracia auténtica. Antoinette Rouvroy proporciona una de las versiones mejor informadas de esta idea:

«El derecho a la privacidad garantiza la posibilidad de un sujeto de pensar de forma diferente a la mayoría y de revisar sus preferencias de primer orden. Por tanto, la privacidad es una condición de la existencia de «sujetos» capaces de participar en una democracia conversadora. En consecuencia, la privacidad también protege estilos de vida legales pero poco populares contra las presiones sociales para que se adapten a las normas sociales dominantes. La privacidad, en tanto que ausencia de límites no razonables en la construcción de la propia identidad, sirve para evitar o combatir la «tiranía de la mayoría». El derecho a la privacidad y el derecho a no ser discriminado tienen en común que protegen las oportunidades de que los individuos experimenten una diversidad de formas de vida no convencionales. La privacidad en sí es una herramienta para evitar discriminaciones y prejuicios».[38]

El derecho a la privacidad, por tanto, se puede conceptualizar como un derecho a la integridad contextual que protege la posibilidad que tiene cualquiera de construir su propia identidad a través de relaciones diferenciadas. El objetivo de este «derecho a la diferencia» es garantizar la multiplicidad, la creación, la novedad y la invención en una sociedad democrática y evitar el inmovilismo o una fuerte normalización estéril. Por eso, la descontextualización de la información personal se puede considerar como una de las amenazas principales para el derecho a la privacidad.

34. J. JAMES (1975). «Why Privacy Is Important». *Philosophy and Public Affairs*, vol. 4, n.º 4, págs. 323-333.
35. P. E. AGRE; M. ROTENBERG (eds.) (1998). «Technology and Privacy. The New Landscape». *MIT Press*. Pág. 3.
36. Véase, p. ej. A. ROUVROY; Y. POULLET (2009). «The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy». En: S. GUTWIRTH; P. DE HERT; Y. POULLET (eds.). *Reinventing Data Protection*. Springer.
37. Véase ECHR (febr., 2003). *Odièvre v. France*, donde el tribunal reconoció que el derecho a la privacidad (artículo 8 de la Convención Europea sobre Derechos Humanos) protege, entre otros intereses, el derecho al desarrollo personal.
38. A. ROUVROY (2008). «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence». *Studies in Ethics, Law, and Technology*, vol. 2, n.º 1, pág. 34.

Esta amenaza de descontextualización está particularmente presente en el caso de Facebook, dado que es una plataforma de contextos colapsados. De hecho, el servicio funde cualquier relación posible en un único espacio social: amistad, política, trabajo, amor, *etc.*, todas se mezclan en un entorno único. Por tanto, se puede considerar que Facebook es lo que Foucault denomina heterotopía. Según el filósofo,

«Las heterotopías son anti-sitios, una especie de utopía hecha realidad en la que los sitios reales, todos los demás sitios reales que se pueden encontrar en una cultura, se representan, objetan e invierten simultáneamente. Los lugares como éste están fuera de cualquier lugar, aunque sea posible indicar su ubicación en la realidad».[39]

Esta definición, aplicada a Facebook, revela toda su precisión. De hecho, los servidores de Facebook están situados en algún lugar de EE.UU., por lo que se puede indicar su ubicación en la realidad.Además, al igual que las heterotopías, Facebook «*puede yuxtaponer en un único lugar real varios lugares incompatibles entre sí*».[40] En este sentido, se puede considerar que Facebook está fuera de todos los lugares. De hecho, mientras en el mundo físico las puertas regulan la entrada, los muros amortiguan el sonido, las cortinas bloquean las miradas curiosas, mientras podemos modular el volumen de nuestra voz durante una conversación dependiendo de cuán delicado sea el contenido y quién pueda oírlo, la arquitectura «descontextualizadora» de Facebook está por encima del espacio y, por tanto, dificulta en gran medida ajustar nuestra presentación para adecuarla a diferentes situaciones.[41] Por tanto, la arquitectura heterotópica de Facebook tiene el potencial de generar una asimetría entre la audiencia que imagina un usuario y su audiencia real, simplemente porque la plataforma carece de separación de espacios. Con ello, el servicio dificulta aún más a los usuarios la evaluación de qué normas contextuales de adecuación o distribución deberían esperar que se respeten cuando se divulga información en el sitio.

Es aquí donde el fenómeno de la descontextualización en Facebook amenaza el derecho a la privacidad: amenaza la posibilidad del ser humano de actuar como un yo contextual y relacional y le impide construir su propia identidad a través de relaciones diferenciadas. Con ello, Facebook también puede causar discriminaciones y prejuicios importantes.

2.2. Consecuencias de la amenaza de la descontextualización sobre la protección de datos como un derecho de los sujetos de datos

El fenómeno de la descontextualización en Facebook no sólo amenaza al derecho a la privacidad de los seres humanos, sino también al derecho a la protección de datos de los «sujetos de datos». De hecho, aunque el derecho a la privacidad trata sobre seres humanos, los instrumentos más importantes de protección de datos crean derechos para «sujetos de datos». La directiva 95/46 define un «sujeto de datos» como una persona natural identificada o identificable y a una «persona identificable» como una que se puede identificar, directa o indirectamente, sobre todo con referencia a un número de identificación o a uno o varios factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. Así, un «sujeto de datos» se concibe como alguien que se puede identificar sobre la base de uno o varios factores específicos de *un aspecto* de su identidad. Por eso, Agre define el derecho a la protección de datos como *«el derecho a controlar un aspecto de la identidad que uno proyecta hacia el mundo».*[42] Es interesante que el derecho a la protección de datos se pueda considerar una forma de control sobre una proyección *parcial* de la «identidad» de uno, que, como ya se ha mencionado, es extremadamente *contextual* y *relacional*.

Por este motivo, creo que el derecho a la protección de datos se puede conceptualizar como un derecho otorgado a «dividuos». Registrado desde que se publicara el primer Diccionario de Noah Webster (1828) hasta la actualidad, el término «dividuo» significa «*dividido, compartido o participado, en común con otros*». El Random House Unabridged Dictionary ofrece los siguientes significados: 1) divisible o

39. M. FOUCAULT (1967). «Of Other Spaces». *Heterotopias*.
40. *Ibidem*.
41. Se puede encontrar la misma idea en C. PETERSON (2009). «Saving Face: The Privacy Architecture of Facebook» » (borrador para comentarios – primavera de 2009). *Op. cit.* Pág. 9 y 35.
42. P. E. AGRE; M. ROTENBERG (eds.) (1998). «Technology and Privacy. The New Landscape». *MIT Press*. Pág. 3.

dividido; 2) separado, distinto; 3) distribuido, compartido. Por ende, la palabra «dividuo» implica tanto el significado de «compartido» como el de «dividido», características básicas de las *relaciones contextuales* en las que el contenido «diferenciado» se «comparte» en función de con quién se está comunicando. Asimismo, Deleuze usa el término «dividuo» en su descripción de las sociedades del control *«que ya no operan confinando a los usuarios sino a través del control continuo y la comunicación instantánea»*.[43] Para Deleuze, la sociedad contemporánea ha causado una crisis generalizada en la que los espacios de enclaustramiento convierten a los usuarios en «*dividuos*» de datos. Según el filósofo,

«Las sociedades disciplinarias tienen dos polos: la firma que identifica al individuo y el número o la numeración administrativa que indica su posición dentro de una masa. En las sociedades de control, por otro lado, lo importante ya no es la firma o el número, sino un código: el código es una contraseña de acceso, mientras las sociedades disciplinarias están reguladas por términos de vigilancia (tanto desde el punto de vista de la integración como del de la resistencia). El lenguaje numérico del control está formado por códigos que marcan el acceso a la información o lo deniegan. Ya no nos encontramos tratando con el binomio masa/individuo. Los individuos se han convertido en «dividuos» y las masas en muestras, datos, mercados o bancos.»[44]

Tal como ilustra la cita, una de las características de las sociedades de control es la emergencia de «dividuos» concebidos como «seres humanos corpóreos infinitamente divisibles y reductibles a representaciones de datos mediante las modernas tecnologías de control, como sistemas basados en el ordenador».[45] Tal como escribe Williams, a través de los datos que se obtienen sobre nosotros, las tecnologías de control pueden separar quiénes somos y lo que somos de nuestros yos físicos. Los datos se convierten en representaciones de nosotros dentro de la red de relaciones sociales; los datos son los indicadores de nuestros hábitos y preferencias. Adoptando el término de Laudon, podemos hablar de nuestras «imágenes en datos»:[46] dado que no estamos presentes físicamente, existe el riesgo de que se nos reduzca a nuestros intereses y comportamientos documentados. Tal como indica Williams, *«esto implica el riesgo de que los complejos procesos de autodeterminación se concreten en unas pocas fórmulas en un soporte de almacenamiento electrónico. La separación de nuestros yos y nuestras representaciones trae a la luz un segundo aspecto de nuestra dividualidad. Como datos, somos clasificables de diversas maneras: se nos incluye en diferentes categorías, y se nos evalúa con distintos fines. Por tanto, nuestra divisibilidad pasa a ser la base de nuestra clasificabilidad en categorías delimitadas, útiles e incluso beneficiosas para terceros que manipulan los datos»*.[47] En tercer lugar y de forma fundamental, dada la divisibilidad de nuestras imágenes de datos en varios contextos de representación, los «dividuos contextuales» están cada vez más amenazados por el riesgo de la *descontextualización*. De hecho, dada la extrema fluidez de los datos electrónicos, la información obtenida en un contexto situacional puede ser reutilizada en otro sentido, a veces muy inapropiado.

Teniendo en cuenta estas amenazas diversas que resultan de nuestra creciente divisibilidad, creo que la regulación europea para la protección de datos se diseñó para dotar a los «dividuos» de los medios necesarios para controlar la imagen informativa que proyectan en su «contexto dividual» estableciendo principios generales de protección de datos y proporcionando derechos a los «sujetos de datos». En otras palabras, los «sujetos de datos» se pueden considerar «dividuos» con medios legales para desafiar a cualquier descontextualización de la información procesada sobre ellos. Se pueden encontrar ejemplos concretos de sus medios con relación a su imagen informativa contex-

43. G. DELEUZE (oct., 1992). «Postscript on the Societies of Control». *MIT Press*. Cambridge, MA. Págs. 3-7. Disponible en: http://www.spunk.org/texts/misc/sp000962.txt
44. *Ibidem*.
45. R. W. WILLIAMS (2005). «Politics and Self in the Age of Digital Re(pro)ducibility». *Fast Capitalism*, vol. 1, n.º 1. Disponible en: http://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html
46. Véase L. KENNETH (1986). *The Dossier Society: Value Choices in the Design of National Information Systems*. Nueva York: Columbia U.P.
47. R. W. WILLIAMS. *Op.cit*.

tual en la Directiva 95/46. En primer lugar, y lo más importante, el artículo 6 obliga al procesamiento de datos *«con fines especificados, explícitos y legítimos y no se podrán procesar más allá de ningún modo incompatible con estos fines»*. En cierto sentido, el principio de limitación de fines conecta una protección adecuada para los datos personales con las normas de información de los contextos específicos, exigiendo a los controladores de datos que estos datos no se *distribuyan* más allá cuando este nuevo flujo no respete las normas contextuales. El mismo artículo de la Directiva también requiere que los datos sean *«adecuados, relevantes y no excesivos con relación al fin para el que se obtienen y/o procesan»*, exigiendo que la obtención y difusión de la información sean *adecuadas* para ese contexto y obedezcan las normas de información aplicables en él. Estos dos principios de la Directiva Europea (limitación de los fines y calidad de los datos) se pueden interpretar como la consagración de la teoría de Helen Nissembaum, según la cual *«una normativa sobre la privacidad en términos de integridad contextual afirma que se ha producido una violación de la privacidad cuando se incumplen las normas contextuales de adecuación o de distribución»*.[48] En consecuencia, los derechos de información, acceso, rectificación y oposición se pueden considerar medios legales de atribución a «dividuos contextuales» para que se enfrenten a cualquier incumplimiento de las normas contextuales (de adecuación o distribución) por parte de los controladores de datos.

En resumen, mientras el derecho a la privacidad garantiza al ser humano la posibilidad de contar con muchas facetas y actuar de forma contextualmente diferente a fin de asegurar la perseverancia de una democracia vívida y que permita el debate, el derecho a la protección de datos se puede considerar una herramienta para dotar a los «dividuos contextuales» de medios para asegurar la integridad contextual de su imagen informativa.

A mi parecer, conceptualizar el derecho a la protección de datos como derecho de «dividuos contextuales» puede ayudarnos a entender por qué el fenómeno de la descontextualización es tan especialmente dañino para nuestros derechos de protección de datos en un sitio como Facebook. De hecho, uno de los principales efectos de los entornos heterotópicos como Facebook es la *recomposición* artificial de los individuos. Citando a Foucault,

«No se debe concebir al individuo como una especie de núcleo elemental, un átomo primitivo, un material múltiple e inerte sobre el que se aplica energía o con la que parece colisionar y, al hacerlo, se fragmenta o subdivide a los individuos. De hecho, uno de los efectos primordiales de la energía es que ciertos cuerpos, ciertos gestos, ciertos discursos, ciertos deseos se identifican y constituyen como individuos. El individuo, por tanto, no es el vis-a-vis de la energía, es, en mi opinión, uno de sus efectos primordiales».[49]

En Facebook, la información personal que publica un usuario, combinada con los datos que perfilan las acciones e interacciones de los usuarios con otras personas, puede crear un perfil muy rico de los intereses y actividades de esa persona. La recogida multi-contextual de todas mis contribuciones y las de mis amigos puede generar fácilmente una imagen *individual* de mí. Por tanto, al fusionar todos los contextos posibles en un único entorno de información, Facebook niega la existencia de nuestras dividualidades y, en consecuencia, niega nuestros derechos como dividuos.

En otras palabras, la finalidad descrita en la página principal de Facebook –*«Facebook te ayuda a comunicarte y compartir tu vida con las personas que conoces»*– es excesivamente amplia como para determinar qué datos son adecuados, relevantes y no excesivos con relación a dicha finalidad. Si la arquitectura de Facebook elimina la integridad contextual, es porque las características más fundamentales de su diseño entran directamente en conflicto con las normas de distribución y adecuación. De hecho, la multi-contextualidad global no se puede cubrir con un derecho a la protección de datos porque, cuando la finalidad de un servicio se define como «todo», todos los datos se pueden considerar adecuados, relevantes y no excesivos y cualquier distribución ulterior se puede considerar compatible.

48. H. NISSENBAUM (2004). «Privacy as Contextual Integrity». *Washington Law Review*, vol. 79, n.º 1, pág.138.
49. M. FOUCAULT. «Body/Power». En: Colin GORDON (ed.). *Foucault on Power/Knowledge: Selected Interviews and other writings 1972-1977*. Londres: Harvester Press / Nueva York: Pantheon Books. Pág. 91.

Conclusión

El fenómeno de descontextualización en Facebook constituye, con certeza, una amenaza importante tanto para el derecho a la privacidad como para el derecho a la protección de datos. Los legisladores europeos tienen un punto de vista similar. De hecho, en su reciente opinión «sobre el establecimiento de redes sociales virtuales», el Grupo sobre Protección de Datos del artículo 29 señaló que una de sus preocupaciones clave era *«la difusión y el uso de la información disponible en los sistemas de redes sociales para otros fines secundarios e involuntarios»*.[50] Para evitar la descontextualización de la información en los sistemas de redes sociales virtuales, el Grupo sobre la Protección de Datos aboga por una *«seguridad robusta y configuraciones por defecto que salvaguarden la privacidad»*[51] pero también quiere aumentar la responsabilidad de los usuarios imponiéndoles las obligaciones de un controlador de datos cuando se usa el sistema de redes sociales virtuales como *«plataforma de colaboración para una asociación o empresa»,* donde el sistema de redes sociales virtuales se usa principalmente *«como plataforma para impulsar objetivos comerciales, políticos o benéficos»* , cuando el *«acceso a la información del perfil se amplía más allá de los contactos seleccionados por el usuario»* o cuando *«los datos son codificables por los programas de búsqueda»*. Además, según el Grupo sobre Protección de Datos, *«un gran número de contactos podría ser indicativo de que la excepción doméstica no es aplicable y, por tanto, de que el usuario sería considerado un controlador de datos»*.[52]

Dado que solo el 20% de los usuarios toca alguna vez sus ajustes de privacidad,[53] estoy convencido de que unos ajustes de privacidad por defecto más restrictivos constituirían una primera garantía contra la descontextualización. Dicho esto, albergo más dudas sobre la segunda propuesta del Grupo sobre Protección de Datos. De hecho, incrementar las responsabilidades de los usuarios con la esperanza de que se reducirá la descontextualización supone unos niveles elevados de conciencia y conocimiento en los usuarios. Sin embargo, la conciencia sobre los derechos y obligaciones en materia de protección de datos entre los ciudadanos parece seguir siendo bastante escasa. De hecho, según un reciente Eurobarómetro, *«a pesar de los drásticos cambios tecnológicos producidos en las dos últimas décadas, el nivel de preocupación sobre la protección de datos prácticamente no ha cambiado»*.[54] Los mayores niveles de concienciación sobre la existencia de los derechos de protección de datos se encontraron en Polonia (43%), seguidos de Letonia (38%), Francia y Hungría (ambas con el 35%). Menos de uno de cada cinco ciudadanos de Suecia (16%) y Austria (18%) dijeron ser conscientes de las posibilidades legales con que cuentan para controlar el uso de sus propios datos personales.[55]

Por este motivo, y porque es importante para el Tribunal Europeo de Derechos Humanos *«que se interprete y aplique de modo que su salvaguarda sea práctica y efectiva, en lugar de teórica e ilusoria»*,[56] sinceramente creo que la protección de la privacidad y la protección de datos en Facebook no se debe centrar únicamente en las soluciones y penalizaciones para los individuos agraviados sino en el diseño de una arquitectura que rija los flujos de datos multi-contextuales en el sitio. Dada la importancia de la amenaza de la «descontextualización», la arquitectura de Facebook debe estar diseñada de modo que evite cualquier interferencia tanto con el derecho a la privacidad como con la protección de datos, siempre que dicha interferencia no sea estrictamente «necesaria en un estado democrático».

50. Grupo sobre Protección de Datos del artículo 29, opinión 5/2009 sobre el establecimiento de redes sociales virtuales, 12 de junio de 2009, pág. 3.
51. *Ibidem*.
52. *Ibidem*. Pág. 4.
53. Según el director de proyectos de Facebook, Chris Kelly, sólo el 20% de los usuarios modifica alguna vez sus ajustes de privacidad. Véase Randall STRESS (marzo, 2009). «When Everyone's a Friend, Is Anything Private?». *The New York Times*. Disponible en:
http://www.nytimes.com/2009/03/08/business/08digi.html
54. Véase RAPID PRESS RELEASE (abril, 2008). «Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection». *IP*/08/592.
55. Véase el EUROBARÓMETRO (febr., 2008). «Protección de datos en la Unión Europea: la percepción de los ciudadanos» (Informe analítico). Disponible en:
http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
56. Véase el TRIBUNAL EUROPEO DE DERECHOS HUMANOS (mayo, 1980). *Artico v. Italy*. Serie A n.º 37, págs. 15-16, § 33. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (2002). *Stafford v. the United Kingdom* [GC]. N.º 46295/99, § 68-IV.

Para lograr este objetivo, las autoridades europeas podrían incrementar la responsabilidad de los operadores de los sitios de establecimiento de redes sociales haciéndoles responder del diseño de sus sitios. Estos mecanismos ya existen en lo tocante al equipamiento de terminales en el contexto de las comunicaciones electrónicas. De hecho, según el artículo 14(3) de la Directiva 2002/58, *«cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales»*. Del mismo modo, el artículo 3(3)(c) de la Directiva 1995/5 establece que *«la Comisión podrá decidir que los aparatos dentro de ciertas clases de equipamiento o los aparatos de algún tipo en particular se construyan de modo que incorporen salvaguardas a fin de asegurar la protección de los datos personales y la privacidad del usuario y del suscriptor»*.

Con esto, las autoridades Europeas podrían imponer un contenido menos multi-contextual en los sistemas de establecimiento de redes sociales virtuales al requerir a los operadores de dichos sitios que diseñaran su arquitectura de acuerdo con las intenciones específicas de cada usuario. A modo de ejemplo, antes de que un usuario se registre en Facebook, se podría plantear una pregunta como *«¿Con qué fin pretende usar Facebook?»* con una lista de respuestas como «Fin comercial», «fin político», «búsqueda de pareja», «relaciones laborales», «amistad en el mundo real», etc. Una vez determinado con mayor precisión el propósito del registro de cada usuario, Facebook debería obtener únicamente datos adecuados, relevantes y no excesivos con relación a ese fin. Si un usuario desea usar el servicio con múltiples propósitos, debería recomendarse el uso de múltiples cuentas. De un modo más general, los operadores de Facebook deberían considerar cuidadosamente *«si pueden justificar el hecho de obligar a sus usuarios a actuar con su identidad real en lugar de con un pseudónimo»*.[57] En los casos en que el propósito específico del uso no requiere el nombre real, se debería recomendar el uso de pseudónimos.

La reconstrucción de lugares dentro de Facebook es una necesidad absoluta para que los usuarios evalúen qué normas contextuales de distribución y adecuación pueden esperar. Esta reclamación no sólo es útil para respetar la dividualidad de cada usuario en cuanto a su derecho a la protección de datos. De un modo más fundamental, es esencial para permitir a los usuarios construir su identidad como seres múltiples y relacionales y actuar, por ende, como seres humanos.

Cita recomendada

DUMORTIER, Franck (2009). «Facebook y los riesgos de la "descontextualización" de la información». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

<Dirección electrónica del PDF>

ISSN 1699-8154

57. Grupo sobre Protección de Datos del artículo 29, opinión 5/2009 sobre el establecimiento de redes sociales virtuales, 12 de junio de 2009, pág. 11.

Sobre el autor

Franck Dumortier
Franck.dumortier@fundp.ac.be

Franck Dumortier es investigador senior en el CRID (Centro de Investigaciones en Informática y Derecho) y, desde 2005, asistente de derecho en las facultades universitarias de Notre Dame de la Paix en Namur. Sus estudios se centran particularmente en la interpretación del derecho con relación a la vida privada, en lo que se refiere a el uso de las nuevas tecnologías tales como la identificación por radiofrecuencia (RFID), la biometría, la vídeo-vigilancia o incluso las redes sociales virtuales.

Université de Namur
Centre de recherche informatique et droit (CRID)
Rempart de la Vierge 5,
B-5000 Namur, Bélgica